Universal Serial Bus (USB) Checklist
for
Sharing Peripherals Across the Network (SPAN) Security Technical Implementation Guide
Version 1 Release 1

06 January 2006

Developed by DISA for the DOD

Database Reference Number: ______________________________

Database entered by: _________________ Date: _____________

Technical Q/A by: ____________________Date: _____________

Final Q/A by: _______________________ Date: _____________

CAT I: _____

CAT II: _____

CAT III: _____

CAT IV: _____

Total: _____

FOUO UNTIL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist
Confidential System = CONFIDENTIAL Checklist
Secret System = SECRET Checklist
Top Secret System = SECRET Checklist

Enclave Reviewer				**Phone**	
Previous SRR	Y N	**Date of Previous SRR**		**S01 Available**	Y N
Number of Current Open Findings					

Site Name	
Address	
Phone	

Position	**Name**	**Phone Number**	**Email**	**Area of Responsibility**
IAM				
IAO				

USB00.001.00 CAT: 3 USB Poweroff Directive in SFUG

8500.2 IA Control: PRRB-1 Category: 6.4 - Training & Certification

Condition(s):

Target(s):

Vulnerability There is no document instructing users that USB devices be powered off for at least 60 seconds prior to being connected to an IS.

Vulnerability Discussion: Because USB devices that contain only volatile memory are designed to withstand minor fluctuations in power they contain some means of maintaining memory for short power interruptions. Users need to ensure that USB devices remain without power for at least 60 seconds when disconnecting them from one IS, and connecting to a different IS to make sure enough time passes for all power to dissipate and the memory erased.
The IAO will ensure that the SFUG or an equivalent document requires that all USB devices be powered off for at least 60 seconds prior to being connected to an IS.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB00.001.00: The reviewer will interview the IAO and view the SFUG, or equivalent documentation, to verify that it is documented that users should remove all power from a USB device when it is moved from one IS to another for at least 60 seconds to allow all power to dissipate and the memory to erase.

Fix(es): SPAN USB00.001.00: Update the SFUG, or an equivalent document, to include this information.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB01.001.00 CAT: 2 USB MP3 Players Camcorders and digital cameras

8500.2 IA Control: DCBP-1 Category: 2.1 - Object Permissions

Condition(s):

Target(s):

Vulnerability MP3 players, camcorders, or digital cameras are being attached to ISs without prior DAA approval.

Vulnerability Discussion: These devices contain non-volatile memory and could be used to infect an IS which they are attached with malicious code or they could be used to transport sensitive data leading to the compromise of the data. Finally there is normally no DOD requirement for these devices to be attached to a DOD asset.
The IAO, SA, and user will ensure that MP3 players, camcorders, or digital cameras are not attached to ISs without prior DAA approval.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB01.001.00: The reviewer will interview the IAO to verify that the IAO knows that USB devices such as MP3 players, camcorders, or digital cameras are not to be attached to ISs without prior DAA approval, and that this information is disseminated to all users.

Fix(es): SPAN USB01.001.00: The IAO will be made aware of the policy that USB devices such as MP3 players, camcorders, or digital cameras are not to be attached to ISs without prior DAA approval. The IAO will disseminate the policy to all users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB01.002.00 CAT: 2 USB Devices Without Prior Approval

8500.2 IA Control: DCBP-1 Category: 12.4 - CM Process

Condition(s):

Target(s):

Vulnerability USB devices are attached to a DOD IS without prior IAO approval.

Vulnerability Discussion: The IAO needs to be aware of what type of USB devices are being attached to DOD ISs and needs to stop prohibited devices from being attached. By requiring the IAO to approve the USB devices the IAO will be informed.
The IAO or SA will ensure that no USB device is attached to a DOD IS unless approved by the IAO.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB01.002.00: The reviewer will interview the IAO or SA to verify that prior approval by the IAO is required before USB devices are attached to DOD ISs and that this policy is disseminated to all users.

Fix(es): SPAN USB01.002.00: The IAO will know that approval by the IAO is required before USB devices are attached to DOD ISs and the IAO will ensure that this policy is disseminated to all users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB01.003.00 CAT: 2 USB Disguised Jump Drives

8500.2 IA Control: DCBP-1 Category: 5.9 - Device Locations

Condition(s):

Target(s):

Vulnerability Disguised jump drives are not banned from locations containing DOD ISs.

Vulnerability Discussion: Since they could easily be overlooked in a spot search to verify that no restricted or sensitive information is being removed from a location, disguised USB jump drives will be banned from locations containing DOD ISs.
The IAO, SA, and user will ensure disguised jump drives are not permitted in locations containing DOD ISs.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB01.003.00: The reviewer will interview the IAO to verify that the policy banning disguised jump drives from locations containing DOD ISs is disseminated to all users.

Fix(es): SPAN USB01.003.00: Disseminate the policy banning disguised jump drives from locations containing DOD ISs to all users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB01.004.00 CAT: 2 USB Notice of Disguised Jump Drive Ban

8500.2 IA Control: DCBP-1 Category: 11.6 - Warning Banners

Condition(s):

Target(s):

Vulnerability Notices are not prominently displayed informing everyone of the ban of disguised jump drives.

Vulnerability Discussion: Without a notice being posted, users could violate the ban and protest the seizer of the devices.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB01.004.00: The reviewer will interview the IAO and view the notices.

Fix(es): SPAN USB01.004.00: Post the required notices informing people entering a location containing DOD ISs that disguised USB jump drives are banned

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB01.005.00 CAT: 2 USB Persistent Memory DODD 5200-1-R Treatment

8500.2 IA Control: PECS-1: PECS-2: PEDD-1 Category: 11.4 - Disposition

Condition(s):

Target(s):

Vulnerability Persistent memory USB devices are not treated as removable media and contrary to DODD 5200.1-R; the devices are not secured, transported, and sanitized in a manner appropriate for the classification level of the data they contain.

Vulnerability Discussion: Persistent memory USB devices can function as removable media. They have the same vulnerabilities as floppy disk but greater capacity. They will be secured, transported and sanitized as required by DODD 5200-1-R in a manner appropriate for the classification level of the data they contain.
The IAO, SA, and user will ensure that persistent memory USB devices are treated as removable media and, in accordance with DODD 5200.1-R; the devices are secured, transported, and sanitized in a manner appropriate for the classification level of the data they contain.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB01.005.00: The reviewer will interview the IAO to verify that the policy for treating persistent memory USB devices as removable media, and in accordance with DODD 5200.1-R; the devices are secured, transported, and sanitized in a manner appropriate for the classification level of the data they contain is disseminated to all users. This would include any device with internal non-removable persistent memory not just jump drives or disk driver.

Fix(es): SPAN USB01.005.00: Disseminate the policy requiring that persistent memory USB devices will be treated as removable media and, in accordance with DODD 5200.1-R; the devices will be secured, transported, and sanitized in a manner appropriate for the classification level of the data they contain.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB01.006.00 CAT: **2** Persistent Memory USB Devices Labeled

8500.2 IA Control: ECML-1 Category: 11.5 - Device Labels

Condition(s):

Target(s):

Vulnerability Persistent memory USB devices are not labeled in accordance with the classification level of the data they contain.

Vulnerability Discussion: If the persistent memory USB device is not labeled with the appropriate classification level this can lead to the compromise of sensitive data or the compromise of an IS that the device is attached.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB01.006.00: The reviewer will interview the IAO or SA to verify that the labeling of persistent memory USB devices is in accordance with the classification level of the data they contain.

Fix(es): SPAN USB01.006.00: Label persistent memory USB devices in accordance with the classification level of the data they contain. Disseminate this policy to all users.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB01.007.00 CAT: **2** Unencrypted Sensitive Data

8500.2 IA Control: ECCR-1: ECCR-2 Category: 8.2 - Encrypted Data at Rest

Condition(s):

Target(s):

Vulnerability Sensitive data stored on a USB device with persistent memory, that the data owner requires encryption is not encrypted using NIST-certified cryptography.

Vulnerability Discussion: If the data owner believes that the data requires encryption it will be encrypted when at rest. If it is not encrypted this can lead to the compromise of sensitive data.
The IAO, SA, and user will ensure that all sensitive data stored on a USB device with persistent memory, if required by the data owner, is encrypted using NIST-certified cryptography.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB01.007.00: The reviewer will interview the IAO to verify that all sensitive data stored on a USB device with persistent memory, if required by the data owner, is encrypted using NIST-certified cryptography.

Fix(es): SPAN USB01.007.00: Establish a process that will disseminate the requirement for encrypt of sensitive data that the data owner designates as needing encryption. Also establish a process identifying which data needs to be encrypted and notifying the users that the identified data needs encryption.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB01.008.00 CAT: 2 USB Format for Access Controls

8500.2 IA Control: DCBP-1 Category: 2.1 - Object Permissions

Condition(s):

Target(s):

Vulnerability USB devices with persistent memory are not formatted in a manner to allow the application of Access Controls to files or data stored on the device.

Vulnerability Discussion: Without using a format that allows the application of access controls to the device files stored on the USB device may be accessed from any system that the device is connected to.
Note that access controls are easily bypassed on USB devices so this should not be considered an adequate replacement for encryption.
The IAO, SA, and user will ensure that USB devices with persistent memory are formatted in a manner to allow the application of Access Controls to files or data stored on the device.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB01.008.00: The reviewer will interview the IAO to verify that USB devices with persistent memory are formatted in a manner to allow the application of Access Controls to files or data stored on the device. For devices used on a Windows system this would be an NTFS format.

Fix(es): SPAN USB01.008.00: Develop a process to disseminate the requirement that USB devices with persistent memory will be formatted in a manner to allow the application of Access Controls to files or data stored on the device.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB01.009.00 CAT: 2 USB SFUG Section

8500.2 IA Control: PRRB-1 Category: 6.4 - Training & Certification

Condition(s):

Target(s):

Vulnerability There is no section within the SFUG, or equivalent documentation, describing the correct usage and handling of USB technologies.

Vulnerability Discussion: The Security Features User Guide gives the user a single reference for information on the current general and site policies and procedures describing their security responsibilities. The lack of this reference could lead to the compromise of sensitive data.
The reviewer will interview the IAO and review the relevant document. What needs to be here is a description for handling, and labeling of USB devices. Additionally an explanation of the restrictions placed on attaching non-government owned USB devices to a government owned IS and the prohibition of disguised USB jump drives.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB01.009.00: The reviewer will interview the IAO and review the relevant document. What needs to be here is a description for handling, and labeling of USB devices. Additionally an explanation of the restrictions placed on attaching non-government owned USB devices to a government owned IS and the prohibition of disguised USB jump drives.

Fix(es): SPAN USB01.009.00: Develop, update, and distribute a SFUG section dealing with USB devices in accordance with the SPAN STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB01.010.00 CAT: 3 USB SFUG Persistent Non-Removable Memory

8500.2 IA Control: PRRB-1 Category: 6.4 - Training & Certification

Condition(s):

Target(s):

Vulnerability The USB usage section of the SFUG, or equivalent document, does not contain a discussion of the devices that contain persistent non-removable memory.

Vulnerability Discussion: Without a discussion of tthe devices that contain persistent non-removable memory, an uninformed user can mistakenly attach such a device to an IS leading to the denial of service caused by an infection of the IS and possibly the network with malicious code. Additionally the user might compromise sensitive data thinking that removal of a memory card removed all the persistent memory within a device.
The IAO will ensure that the USB usage section of the SFUG contains a discussion of the devices that contain persistent non-removable memory.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB01.010.00: The reviewer will interview the IAO and review the relevant documentation. The discussion should point out that with some devices it may not be obvious that it contains persistent non-removable memory and that, if there is a doubt, it will be treated as if it contains persistent memory.

Fix(es): SPAN USB01.010.00: Develop, update, and distribute a SFUG section on USB devices that discusses devices that may contain persistent non-removable memory in accordance with the SPAN STIG.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes:

USB02.011.00 CAT: 1 An IS BIOS Set to Allow Boot from USB

8500.2 IA Control: DCBP-1 Category: 2.1 - Object Permissions

Condition(s):

Target(s):

Vulnerability An IS has its BIOS set to allow a boot from a USB device.

Vulnerability Discussion: If an IS's BIOS is left set to allow it to be booted from a USB device, an individual can plug a USB device into the IS and force a reboot, either performing a hardware reset or cycling the power, causing whatever operating system is on their USB device. This can lead to a denial of service. Additionally this can lead to the compromise of sensitive data on the IS that was rebooted and possibly to the network the IS is attached.

References: SHARING PERIPHERALS ACROSS THE NETWORK SECURITY TECHNICAL IMPLEMENTATION GUIDE

Checks: SPAN USB02.011.00: The reviewer will interview the IAO or SA to verify that no IS has its BIOS set to allow a boot from any USB device. Note an IS can be booted from a USB device for maintenance or recovery purposes, but will never be allowed to do so when in normal use.

Fix(es): SPAN USB02.011.00: Develop a plan to check all ISs' BIOS settings as soon a possible. The check will verify that none of the BIOS are set to allow a boot from a USB device. Obtain CM approval for the plan and execute the plan.

OPEN: □ **NOT A FINDING:** □ **NOT REVIEWED:** □ **NOT APPLICABLE:** □

Notes: